THEODORE J. BOUTROUS JR., SBN 132099
tboutrous@gibsondunn.com
RICHARD J. DOREN, SBN 124666
rdoren@gibsondunn.com
DANIEL G. SWANSON, SBN 116556
dswanson@gibsondunn.com
JAY P. SRINIVASAN, SBN 181471
jsrinivasan@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

VERONICA S. MOYÉ (Texas Bar No. 24000092; appearance *pro hac vice*)
vlewis@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
2100 McKinney Avenue, Suite 1100
Dallas, TX 75201
Telephone: 214.698.3100
Facsimile: 214.571.2900

MARK A. PERRY, SBN 212532
mperry@gibsondunn.com
CYNTHIA E. RICHMAN (D.C. Bar No. 492089; *pro hac vice*)
crichman@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

ETHAN D. DETTMER, SBN 196046
edettmer@gibsondunn.com
ELI M. LAZARUS, SBN 284082
elazarus@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant, APPLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

EPIC GAMES, INC.,

Plaintiff, Counter-defendant,

v.

APPLE INC.,

Defendant, Counterclaimant.

CASE No. 4:20-cv-05640-YGR-TSH

DEFENDANT APPLE INC.'S RESPONSE TO COURT ORDER RE: OBJECTIONS TO EXPERT TESTIMONY

The Honorable Yvonne Gonzalez Rogers

Pursuant to Pretrial Order No. 6, Dkt. 521, Apple Inc. sets forth below the requested response to Epic's objections to the written direct testimony of Apple's expert, Dr. Aviel D. Rubin. Apple would be pleased to submit a narrative response to Epic's objections if it would aid the Court.

Paragraph of Written Direct Testimony Objected to	**Corresponding Paragraph in Expert Reports**
Dr. Rubin	
¶ 7: **Opinion 6.** The introduction of alternative app stores on iOS devices would jeopardize the security, safety, and trustworthiness of the iOS platform. Many other distribution sources simply will not prioritize security, safety, and trustworthiness. We know this because outside of the iOS platform, there exist stores that primarily traffic in adult content, malware, and/or pirated software. Even distribution sources that mean well would have trouble meeting the standards of Apple's App Review. Some of them will lack the resources to build the various tools and employ the reviewers that Apple currently has on staff. Others will lack the incentives. For example, developers and third-party stores whose financial model depends largely on ad revenues will have less incentive to protect user privacy because much of ad revenue is based on the ability of advertisers to target and know intimate details about end users. And finally, all other sources will lack Apple's knowledge of iOS and iPhone hardware and their security vulnerabilities, as well as the extensive body of knowledge that Apple has accumulated from more than a decade of app review and analysis of threats posed by apps. Internal knowledge of iOS and iPhone architecture cannot be simply revealed to third parties because of the potential associated security threats.	¶ 33: … **Clickware/Clickfraud - A subset of malware that repeatedly clicks on an advertisement to drive up revenue for the host** site or to drain revenue from the advertiser. ¶ 72: Apple has adopted "a multilayered approach to try to keep the iPhone reliable and secure for [Apple's] customers." Apple's App Store provides three types of review in the App approval process: static, dynamic, and manual. I will first discuss static and dynamic reviews which are automated reviews; I will then describe their limitations and how they motivate the need for manual review. It is the manual app review that distinguishes Apple's App Store above all other marketplaces. **Moreover, as C.K. Haun, the Senior Director of Developer Technical Services at Apple, testified, Apple uniquely positioned to conduct this review process; it cannot be farmed out to third parties, as "Apple uses its knowledge of its hardware in the review process and . . . other organizations may not have that knowledge."** ¶ 78: **Certain usability issues, such as advertising volume and placement, are also analyzed by a human reviewer. Human reviewers can identify whether there is excessive advertising on an app**, or whether an app in the children's category includes third-party analytics or third-party advertising that may violate the App Store Review Guidelines' privacy policies. These sorts of violations can be easily identified by humans, but they pose a problem for automated algorithms. Notably, Epic also uses human processes to foster a better user experience. Mr. Sweeney in his deposition explained that "most of our human processes are

	focused on ensuring that the game works, it can be installed and is generally compatible with the hardware we test on." ¶ 87: It is also my opinion that it is necessary for the safety of users, and to ensure that the App Store remains a useful platform for developers, for Apple itself to conduct the iOS app review process. **Even if a third-party reviewer might choose to operate under the same App Store Review Guidelines that uphold high security and privacy standards, Apple reviewers still have a better overall understanding of the iOS ecosystem and can implement and coordinate the review process more effectively.** ¶ 87.b: **Apple reviewers are able to perform certain review tasks based on accumulated internal learnings of the iOS ecosystem, which third-party reviewers lack.** For example, Mr. Haun testified that third-party reviewers would be unable to comprehensively identify whether private APIs are being used in an app. The App Store Review Guidelines forbid the use of private APIs because they may be "designed for a very narrow use" or the use of such APIs could "expose privacy or security risks to a customer"; however, Apple reviewers are able to identify private APIs based on an internal enumeration of all private APIs—confidential information that has not been disclosed to the public. Apple reviewers might also utilize internal review tools tailored to identify private APIs in an app, similar to the tools mentioned in the previous paragraph. ¶ 123: Apple is committed to ensuring that all developers are treated fairly. As Tim Cook describes, "[w]e make an App Store that is for the 1.8 million apps that are on the store . . . we have to have a set of rules the apply to everyone." **Allowing Epic to distribute the Epic Games Store on iOS could force Apple to need to allow another third-party app store to likewise distribute apps. In doing so, users would be put to risk, and it would be incredibly difficult for Apple to guarantee that every third-party app store operates with integrity and the highest of security and privacy standards.** ¶ 178: Drs. Lee and Mickens also do not address many of the negative consequences for security

	that would arise under their proposals, and if Apple did not perform its App Review process and other security protections. In regards to iOS SDKs, Drs. Lee and Mickens do not acknowledge that a less regulated SDK landscape would potentially bring harm to iOS user privacy. As Dr. Lee describes in his report, **third-party advertising SDK YouMi led to apps covertly acquiring user data using private APIs.** Dr. Mickens' on-device security proposals do not and cannot solve these problems as it is exceedingly difficult for on-device security measures to limit the use of private APIs. In addition, Apple requires apps to disclose "all of the data you or your third-party partners collect, unless the data meets all of the criterial for optional disclosure []."; ¶ 216: It also may not be in the best interest of third-party app stores to remove pirated apps from their stores. Because users on non-iOS platforms can easily access stores that host pirated content, these stores have an intrinsic value to users who do not want to pay the full price for apps. **Stores that carry pirated apps can also host advertisements, and since these stores are practically the only places to obtain pirated apps, these stores earn revenue by hosting advertisements on their platform. If these app stores decided to implement strict review processes to prevent pirated games from being uploaded, then users might be less interested in using the stores, which would drive ad revenue down. This in turn means that third-party app stores may not be incentivized to employ a strict app review process.** ¶ 247: Dr. Lee also suggests that third-party stores could achieve the same security goals as the App Store. However, statistics show that third-party app stores host 99.9% of discovered mobile malware. **So, irrespective of whether they would be able to achieve the same security goals, the reality is that they do not.** ¶ 248: **Third-party app stores have different incentives that impact the safety and reliability of their apps. Some third-party app stores may not want to spend their resources on a**

	comprehensive app review process, so they may permit games into their stores even if they are currently in an unreliable state. For example, the videogame Cyberpunk 2077 was released in late 2020 and received immediate criticism for the considerable number of bugs and glitches the game had. After numerous delays, and little to no mention that the game was unstable, the game was released. In the days after release, Sony pulled Cyberpunk 2077 from the PlayStation Store and offered users full refunds because the game was unplayable on certain PlayStation consoles. Other stores, like the Epic Games Store, Steam, and GOG mentioned in Dr. Mickens' report, still let users purchase the game (it should be noted the game ran better on PC but still suffered from numerous bugs). **Cyberpunk 2077 is an example of a game that was released at full price before it had been sufficiently debugged, and it demonstrates how developers may prioritize profit over reliability.** ¶ 251: Other app stores may also permit lower standards of app reliability. Given these examples, **it is clear that different app stores will likely have varying postures of what levels of security, privacy, and reliability are appropriate on their platforms.** ¶ 253: Even Epic's own CEO and app store manager recognize that there will be other app stores with different incentives that run contrary to that of its own app store. This further substantiates my opinion that **Drs. Mickens's and Lee's proposal for alternative third-party app stores would ultimately denigrate Apple's reputation of providing safe and trustworthy apps, and compromise the integrity of Apple's products** (including because users will inevitably allocate some degree of responsibility to Apple). ¶ 297: **Dr. Lee and Dr. Mickens likewise fail to recognize Apple's unique position in conducting a relatively more effective and efficient app review. Apple reviewers have the following resources that are not available to third-party reviewers: (1) Apple's tools specifically tailored for app review, such as machine learning tools trained with data collected from previous app review analysis;**

	(2) the information garnered through the app review process, including the data collected from the app review process and used to update Apple's machine learning tools; (3) the internal learnings of the iOS ecosystem, including lists of private APIs on iOS; (4) internal processes that enable Apple reviewers to escalate apps for further guidance; and (5) internal processes that enable Apple reviewers to escalate security issues to other Apple departments that can make security and privacy improvements across policies, processes, and products.
¶ 82: Outside of the iOS platform, we know that there currently are distribution sites that specifically traffic in the types of apps—such as pirated apps—that Apple prohibits. If permitted to operate and distribute iOS apps, these stores would have no incentive, and are unlikely to attempt, to duplicate Apple's app review efforts. Even third parties that don't explicitly traffic in illegal and malicious content are unlikely to match Apple's App Review efforts for several reasons.	¶ 62: **Each app submitted for distribution on the iOS App Store is reviewed by Apple to ensure compliance with the App Store Review Guidelines and DPLA, and to verify that the app performs as expected and that it is free of malicious code.** Apple's App Store Review Guidelines are detailed and wide reaching. Not only are they designed to ensure that apps function properly, but they also help promote a high-quality experience for the user. **Because of this diligence in ensuring app quality, iOS consistently scores higher than Android on metrics of user satisfaction and perceived platform quality.** ¶ 87: It is also my opinion that it is necessary for the safety of users, and to ensure that the App Store remains a useful platform for developers, for Apple itself to conduct the iOS app review process. **Even if a third-party reviewer might choose to operate under the same App Store Review Guidelines that uphold high security and privacy standards, Apple reviewers still have a better overall understanding of the iOS ecosystem and can implement and coordinate the review process more effectively.** ¶ 215: … **It is understood that many third-party app stores provide users with pirated versions of apps**…. ¶ 216: **It also may not be in the best interest of third-party app stores to remove pirated apps from their stores. Because users on non-iOS platforms can easily access stores that host pirated content, these stores have an intrinsic**

	value to users who do not want to pay the full price for apps. Stores that carry pirated apps can also host advertisements, and since these stores are practically the only places to obtain pirated apps, these stores earn revenue by hosting advertisements on their platform. **If these app stores decided to implement strict review processes to prevent pirated games from being uploaded, then users might be less interested in using the stores, which would drive ad revenue down. This in turn means that third-party app stores may not be incentivized to employ a strict app review process.**
¶ 84: Second, the incentives of third-party stores may drive them to deliberately adopt a standard lower than Apple's. For example, certain large companies are heavily dependent on ad revenue, which in turn, is heavily dependent on the ability of an app to track user behavior. Other companies may choose to maintain different standards. For example, Apple's App Store Review Guidelines reject apps that alter or disable standard device inputs like device volume buttons, but the Google Play Store's Developer Program Policy does not have a similar requirement. Returning to the Tic-Tac-Toe app example, if it also included an instruction to users to reconfigure their devices to raise the volume on the microphone to enhance listening sensitivity, Google might allow that app for distribution via the Google Play Store where Apple might not. As mentioned earlier, Google similarly does not have guidelines pertinent to privacy protection such as the Apple App Store Review Guidelines that limit background activity to specific functions and restrict the calling of and collection of SMS data. Another example is the GOG app store, which operates on PCs and has a business model of restoring old, unworkable, or unoptimized games. Because GOG's purpose is to make unworkable games work again, not to provide secure apps, it likely prioritizes security less than the App Store.	¶ 33: … **Clickware/Clickfraud - A subset of malware that repeatedly clicks on an advertisement to drive up revenue for the host** site or to drain revenue from the advertiser. ¶ 78: **Certain usability issues, such as advertising volume and placement, are also analyzed by a human reviewer. Human reviewers can identify whether there is excessive advertising on an app**, or whether an app in the children's category includes third-party analytics or third-party advertising that may violate the App Store Review Guidelines' privacy policies. These sorts of violations can be easily identified by humans, but they pose a problem for automated algorithms. Notably, Epic also uses human processes to foster a better user experience. Mr. Sweeney in his deposition explained that "most of our human processes are focused on ensuring that the game works, it can be installed and is generally compatible with the hardware we test on." ¶ 178: Drs. Lee and Mickens also do not address many of the negative consequences for security that would arise under their proposals, and if Apple did not perform its App Review process and other security protections. In regards to iOS SDKs, Drs. Lee and Mickens do not acknowledge that a less regulated SDK landscape would potentially bring harm to iOS user privacy. As Dr. Lee describes in his report, **third-party advertising SDK YouMi led to apps covertly acquiring user data using private APIs.** Dr. Mickens' on-device security proposals do not and

	cannot solve these problems as it is exceedingly difficult for on-device security measures to limit the use of private APIs. In addition, Apple requires apps to disclose "all of the data you or your third-party partners collect, unless the data meets all of the criterial for optional disclosure []. ¶ 216**: It also may not be in the best interest of third-party app stores to remove pirated apps from their stores. Because users on non-iOS platforms can easily access stores that host pirated content, these stores have an intrinsic value to users who do not want to pay the full price for apps.** Stores that carry pirated apps can also host advertisements, and since these stores are practically the only places to obtain pirated apps, these stores earn revenue by hosting advertisements on their platform. **If these app stores decided to implement strict review processes to prevent pirated games from being uploaded, then users might be less interested in using the stores, which would drive ad revenue down. This in turn means that third-party app stores may not be incentivized to employ a strict app review process.** ¶ 248: **Third-party app stores have different incentives that impact the safety and reliability of their apps. Some third-party app stores may not want to spend their resources on a comprehensive app review process, so they may permit games into their stores even if they are currently in an unreliable state.** For example, the videogame Cyberpunk 2077 was released in late 2020 and received immediate criticism for the considerable number of bugs and glitches the game had. After numerous delays, and little to no mention that the game was unstable, the game was released. In the days after release, Sony pulled Cyberpunk 2077 from the PlayStation Store and offered users full refunds because the game was unplayable on certain PlayStation consoles. Other stores, like the Epic Games Store, Steam, and GOG mentioned in Dr. Mickens' report, still let users purchase the game (it should be noted the game ran better on PC but still suffered from numerous bugs). **Cyberpunk 2077 is an example of a game that was released**

	at full price before it had been sufficiently debugged, and it demonstrates how developers may prioritize profit over reliability. ¶ 249: In his report, Dr. Mickens discusses the app store GOG, which optimizes old games prior to distribution. Dr. Mickens frames the distinction between Apple's App Store and GOG's app store as based on their goals to show that different app stores can provide different services that benefit users and developers. However, **Dr. Mickens fails to consider that differences in the app stores' business models can also create diverging incentives that ultimately dictate the security standards of app stores. For instance, GOG's business model is to make old, unworkable or unoptimized games work again. The App Store business model, however, is to check that working apps properly function in ways they are represented to users. Based on my experience, I would expect the former model to prioritize security less than the latter, as it is less critical to the success of the business model.** I understand that Apple's expert, Dr. Rubinfeld, discusses this issue in greater detail and refer to his report. ¶ 317: Android and the Google Play Store provide an instructive example, given that Dr. Mickens implies that "Android is actually more secure than iOS." I disagree. **Earlier, I explained that Google Play Store's review process has been trying to catch up to that of Apple's, such as by adding a certain level of human reviewers to its app review process in 2015, which is approximately 7 years after Apple's app review launched in 2008. Even so, it can still be observed that Google's app approval policy is less restrictive than that of Apple's when it comes to security and privacy aspects. One example being that Apple's App Store Review Guidelines reject apps that alter or disable standard device inputs like device volume buttons, while Google Play Store's Developer Program Policy does not have a similar requirement. An Android app under Google's DPP might deceive users and instruct users to reconfigure their devices.** Missing

	security and privacy requirements like this could be an indication that these aspects are not verified by Google in Google Play Store's Android app review process.

Separately, Apple has objected to paragraphs in the written directs of Prof. Athey, Prof. Mickens, Dr. Cragg, Dr. Evans, and Dr. Lee that have no support in their disclosed reports. In fact, some of the opinions in those paragraphs were affirmatively disavowed by these experts when they were deposed. The chart below indicates, where appropriate, such disavowal.

Paragraph of Written Direct Testimony Objected to	**Corresponding Paragraph in Expert Reports / Relevant Deposition Testimony**
Prof. Athey	
¶¶ 86–96	None
Prof. Mickens	
¶ 94	None
Dr. Cragg	
¶ 26	None
¶¶ 38–39	None
¶¶ 55–56	None
¶¶ 58–59	None
¶¶ 66–68	None
¶ 72	None
¶¶ 97–104	None
Dr. Evans	
¶ 39	None
¶¶ 48–50	None

Dr. Lee	
¶ 19: Dr. Rubin asserts that "[a]ny evaluation of the security of iOS . . . must consider its context, objectives, potential attackers, and the manner in which users use their systems, or the iOS 'threat model'". However, Dr. Rubin's discussion omits any record evidence of Apple's own threat modeling for iOS. The Apple materials I have reviewed do not suggest that Apple's decision to adopt exclusive app distribution on iOS was a result of threat modeling.	Dep. 172:17–173:4 Q: If I wanted to find the section of your report that discusses the threat model for iOS versus MacOS, would I be able to find that? A: **So again, I never said I discussed threat model in my report.** Your question about threat model when I answered it I specifically say that's in the context of security in general, not the narrow context of this case. Q: **Okay. So for the purpose of this case you have not analyzed whether iOS and MacOS face the same threat model; is that accurate?** A: **I don't recall specifically discussing – how to put? Specifically enumerating threats.**
¶ 76	None
¶ 77: Dr. Rubin references several studies that suggest that Android is less secure than iOS, but these studies are also unreliable because 1) the comparisons can only involve identified malware and 2) there are many reasons why platforms may differ in amount of malware beyond the platforms' security capabilities (e.g., demographics or susceptibility of users). It is very difficult to design a comprehensive study to compare the security of different platforms. For example, the Nokia threat intelligence report that Dr. Rubin references to suggest that Android devices are fifty times more likely to be infected with malware than iOS devices does not appear to control for differences in market share among Android and iOS devices. While the statistics show that Android comprises a greater overall percentage of infected devices than iOS, these figures are also driven by each platform's volume share of devices. Even if studies show that Android contains more malware than iOS, in practice, it is very difficult to isolate the effect to nonexclusive distribution.	Dep. 289:16–21 Q: **Do you review the Nokia security report that comes out from time to time?** MR. CLARKE: Objection to form. THE WITNESS: **Again, I don't – I don't recall specific reports.** I do know Nokia being a company, yeah.
¶ 80: Dr. Rubin presents a "parade of horribles" argument, suggesting that iOS	Dep. 221:9–24 Q: In China there is no Google Play store; right?

would resemble the Android platform in China if iOS were to permit third-party app distribution. I disagree with that comparison. First, as noted above, there are unique features of the Android security model that are entirely distinct from iOS. Apple does not have to adopt those features in order to allow for third-party distribution. Second, Dr. Rubin's "case study" of Android in China tacitly attributes all of the security issues he describes to the app distribution channel. But he shows no evidence justifying that attribution and fails to consider other factors affecting that ecosystem—including a much more fragmented Android ecosystem, much cheaper hardware, less sophisticated device makers and other factors. Dr. Rubin's suggestion that enabling third-party distribution on iOS would lead to an ecosystem that mirrors Android in China in this respect is unsubstantiated. Dr. Rubin has performed no formal analysis or comparison that would allow him to make any meaningful conclusions based on the Android market in China.	A: That I don't know. I haven't been to China for many years now, no, I don't know. I don't know for a fact one way or the other. Q: **You don't have an understanding of software distribution in China?** A: **In China specifically, I don't recall.** Q: **You've never made observations about the prevalence of pirated softwares in China?** A: **Not in recent years. Not to memory. Like I said, I haven't been – I haven't been keeping what's going on there for several years now.**
¶ 103: For example, Aptoide is a third-party app store on Android that advertises security as its top priority. It claims to accomplish this through an app review process that includes both a human and an automated review, which is comprised of six different anti-viruses. Once an app has been uploaded to the store, "apps are rescanned over and over to ensure that no malware is missed" and "user input is then used by the security team to update the anti-malware system". As a result of these efforts, a 2017 academic study showed that Aptoide was the safest Android marketplace, safer than even the Google Play Store. Such empirical evidence suggests that third parties indeed have incentives to keep their stores secure, and may even do a better job than the platform operator.	Dep. 107:18–108:9 Q: **By the way, in your report do you identify any existing app distribution store that uses tools that are similar or equivalent to Apple's tools? Is that something that you've identified in your report?** A: Are you referring to – in the context of iOS, right? Q: No. In any context. Any app distribution store. **Do you identify anyone right now that you believe uses a similar quality grade of tools as Apple does?** A: So, I guess my task is to look at the iOS app store review process. **So I wasn't tasked to compare app store with any other app store, so I don't recall specifically comparing other stores – yeah, their behaviors or their mechanism, I don't recall that.**
¶ 104	None

Dated: April 30, 2021

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Mark A. Perry*
Mark A. Perry

Attorneys for Defendant Apple Inc.